REMARKS

The Office Action of 23 June 2010, has been received and reviewed. All pending claims stand rejected. Clarifying amendments are to be made to the application as previously set forth. All amendments and claim cancellations are made without prejudice or disclaimer. No new matter has been added. Reconsideration is respectfully requested.

OBJECTED TO CLAIMS:

Responsive to the indications of the Examiner, applicant has amended claims 23 and 24 by rewriting each of the claims in independent form to include therein all of the limitations of their respective base claim and any intervening claim. Furthermore, applicant has amended the language of the claim to obstensibly conform to the requirements set forth in paragraph 2 of the Action. In view of these amendments and the prior indication of the Examiner that these claims would be allowable provided that such amendments were affected, applicant respectfully submits that claims 23 and 24 are now in condition for allowance.

REJECTION UNDER 35 U.S.C. § 102(E)

Claims 1-8 and 10-16 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent 6,327,578 to Linehan. The applicants respectfully traverse the rejection.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Brothers v. Union Oil Co. of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The identical invention must be shown in as complete detail as is contained in the claim. *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Furthermore, unless a single prior art reference describes "all of the limitations claimed" **and** "all of the limitations [are] **arranged or combined in the same way** as recited in the claim, it cannot be said to prove prior invention of the thing claimed and, thus, cannot anticipate under 35 U.S.C. § 102." *Net MoneyIN Inc. v. VeriSign Inc.*, 545 F.3d 1359, 1371 (Fed. Cir. 2008) (emphasis added). A single prior art reference must "clearly and unequivocally" describe the claimed invention "without *any* need for picking, choosing, and combining various disclosures not directly related to each other by the teachings of the cited reference." *Id.* (*citing In re Arkley*, 455 F.2d 586, 587 (C.C.P.A. 1972)).

Applicant respectfully submits that there are a number of features of claim 1 that are not disclosed by U.S. Patent No. 7,103,575 (Linehan). Since Claim 1 is the base independent claims for claims 2-8 and 10-16, applicant submits that these distinctions apply equally to the dependent claims as well.

First, in Linehan, there is no disclosure of a secure data entry device that comprises a discrete device with a data transmission output connected to a public data network.

Referring to Linehan at column 10 in the paragraph between lines 21 and 41, it mentions that the consumer's PC 205 is a new component of the present invention. A PC must have a smart card reader, appropriate software, and connectivity via the internet 210 to both a merchant 225 and consumer's issuing bank 220 (or issuer gateway 215). The reader 200 may have a secure PIN keypad; alternatively, PINs may be entered by the PC keyboard. The consumer's PC 205 must act as the POS terminal to the EMV smart card, implementing the functions (e.g., responding to requests from merchant 225), which are needed to make the EMV card work according to the integrated EMV and four-party protocol described herein.

It goes on to say "the PC 205 is under the control of the end user rather than a merchant or bank."

The description of using an alternative PC keyboard in order to enter the PIN shows a significant difference in the definition of "secure" between claim 1 and Linehan.

In Linehan, with reference to Figure 3B in column 11, lines 1 to 46, it mentions at line 4 that the merchant 305 sends data for authentication to the consumer's PC 335. The PC 335 then sends the data for authentication to the smart card 300, which then signs the data and returns it to the consumer's PC 335. The signed dynamic application data is then sent to the issuing bank 350 via issuer gateway 345. No importance is placed on the issuer gateway; it is said that this can be omitted.

At line 34 it mentions that the consumer's PC 335 performs authentication functions similar to merchant POS terminal of the existing EMV. In particular, software in the consumer's PC handles the reception of the merchant's data for authentication, the sending of the data for authentication to the smart card and receiving the signed dynamic application data and sending this to the issuer gateway and receiving a response from the issuer gateway.

Thus, it is the action of the consumer's PC that performs authentication of the merchant data wherein a PIN is entered into the PC and encryption is performed at the PC. At line 56, column 14, it mentions the consumer PC sends an encryption key request to the issuing bank, which then returns an encryption key response that contains a new issuer encryption certificate. The PC verifies the certificate, prompts the user for the PIN using the public key contained in the issuer encryption certificate. The consumer PC includes this encrypted PIN in the four-party authorization request transmitted to the issuing bank in message 710".

This is in contrast to claim 1 in that the secure data entry device is a discrete device that has a data transmission output connected to the public data network. Claim 1 has the features of the secure data entry device, which includes means for the user to enter identifying information of a card issued by the financial institution, means for the user to enter the user's PIN, means for encrypting the identifying information and PIN for secure transmission and means for transmitting the encrypted identifying information and PIN in a secure manner via the data transmission output via the public data network to the gateway device.

Thus, it is clear that the secure data entry device of claim 1 is the sole means for providing encryption of the identifying information and PIN after each are entered on the secure data entry device.

The smart card reader 200 in Linehan suggests simply a reader for reading smart card information. Linehan requires the consumer's PC 205 to provide authentication and encryption of the PIN and card number. As mentioned previously, the fact that an alternative PC keyboard can be used to enter the PIN shows that the identifying information and PIN may not be securely transmitted to the issuer or issuing financial institution.

With the present invention as claimed in claim 1, the authentication system is able to confirm the presence of the actual owner of the card at the point of purchase. This is after the user has entered identifying information of the card, his or her PIN, whereby an approval response is provided to show authentication of the identifying information by a card-issuing financial institution. Furthermore, the system enables the secure data entry device to derive verifiable proof of the presence of the actual owner of the card at the point of purchase that may be used in subsequent transactions with other devices having the ability to verify the proof.

Together, these features show that the device is more than a simple smart card reader that has functionality, which is not present or shown in the device of Linehan.

In claim 1, the feature of a gateway device including means for transmitting identifying information to the card-issuing financial institution and for receiving an approval response from the card-issuing financial institution over a private data network, is not disclosed in Linehan. In Linehan, the existing gateways currently provided by card issuers are used in the patent. This is in contrast to the gateway device of the present invention, which is designed to operate as part of the authentication system and provides unique functionality. Such unique functionality includes means for modifying received payment messages, means for transmitting the modified payment transaction messages to the card-issuing financial institution, all of which are not disclosed by Linehan.

Other differences include that the present invention provides a secure data entry device that can accept card information from any smart card or magnetic stripe card or a user may enter a personal account number using the keypad on the device. In contrast, Linehan only allows the use of ENV-enabled smart cards.

There is no disclosure in Linehan of the feature of the secure data entry device having means for the user to enter identifying information of a card issued by the financial institution nor is there means for the user to enter the user's PIN and means for encrypting the identifying information and PIN for secure transmission. There is no disclosure of means for transmitting the encrypted identifying information and PIN in a secure manner via a data transmission output to a gateway device. This has been described previously.

Furthermore, in column 15, lines 5 to 11, of Linehan it mentions that as an alternative, the encryption key used for on-line PIN processing may be obtained by statically and permanently providing an issuer public key directly in the wallet software. In this case, the wallet would encrypt the on-line PIN using the issuer public encryption key and thereafter the issuer decrypts the PIN using the matching private key.

Thus, Linehan teaches a technique of PIN encryption that is unique to the four-party protocol described in the patent, which is a variation of SET and which is a requirement to the operation of the invention disclosed in Linehan.

The present application as claimed is not subjected to this limitation and encryption of the PIN for verification by the issuing institution can be carried out in several different ways.

Furthermore, the term "gateway" as used in the Linehan document refers to an issuer gateway. Conversely in the present patent application and as claimed, the gateway is used and described solely for the implementation of the authentication system and is not an issuer gateway.

For all of the above reasons, it is considered that claim 1 is novel over Linehan.

In relation to claim 2, this is dependent upon claim 1 and, therefore, includes all of the features of claim 1. As claim 1 is considered to be novel over Linehan, then so too is claim 2.

With regard to claim 3, the personal computer disclosed therein and connected between the public network and secure data entry device is only used for connecting the secure data entry device to the gateway over the public network and does not perform any enabling of trusted transactions, such as authentication or encryption. This is the case with the PC of Linehan, which runs a program that enables a trusted transaction and provides encryption as previously discussed.

With regard to claims 4, 5 and 6, each of these claims are individually dependent upon claim 1. As claim 1 was considered novel over Linehan, then so too claims 4, 5 and 6 are novel over Linehan as they incorporate all of the features of claim 1.

With regard to claims 7 and 8, the secure data entry device incorporates a card reader and also a secure keypad to enable the user to enter data into the system. In Linehan, the card reader and the PC through which data is entered are separate devices. With regard to claim 8, the card reader of the present invention is able to read a number of different types of cards, which is not disclosed in Linehan.

With regard to each of claims 10, 11 and 12, these claims incorporate all of the features of claim 1 and are considered to be novel over Linehan as all of the features of present claim 1 is considered to be novel over Linehan.

With regard to claim 13, the differences between the gateway device as claimed in claim 1 and the issuer gateway of Linehan have been discussed previously.

With regard to claims 14, 15 and 16, the secure data entry device accepts both standard EMV type responses as well as standard non-EMV type responses such as those associated with magnetic stripe card–based transactions or manually entered account number transactions. In contrast, in Linehan there is only described a response from the enquirer gateway relevant for an EMV-based transaction.

Furthermore, the secure data entry device includes means for deriving the approval response verifiable proof that the identifying information of the customer has been authenticated by the card-issuing financial institution. In Linehan, the approval for the EMV-based transactions is done by the user's PC, which is separate to the card reader 200.

With regard to claim 27, similar comments apply to this claim as they do in claim 1. Therefore, claim 27 has novelty over the Linehan document.

In view of these distinctions, applicant respectfully submits that claims 1-8 and 10-16 distinguish over the Linehan reference and therefore the rejections of these claims should be withdrawn.

REJECTION UNDER 35 USC §103:

Claims 17 to 22, 25 and 26 stand rejected under 35 USC §103 as being obvious over the combination of Linehan and Flitcroft et al. Applicant respectfully traverses the rejection.

In Flitcroft, it mentions at paragraph 12 in the background to the invention the development and provision of smart cards, which is said to contribute to credit card security systems by using some encryption system. On page 3 in paragraph 20, it mentions that one of the problems with this type of system is that due to competing technologies and, therefore, a multiplicity of incompatible formats, this will be a disadvantage and a deterrent to traders and consumers. Many of the systems (including smart card-based systems) require modifications of the technology used at the point of sale. This requires considerable investment and further limits the uptake of such systems.

The Linehan system revolves around the use of smart cards for internet commerce and integrates an existing standard, known as the EMV standard, with an augmented four-party credit/debit payment protocol that is disclosed in U.S. Patent No. 6,327,578. Therefore, by providing a known standard to be used with a protocol disclosed in an earlier patent, it is extremely unlikely that the skilled person would refer to Flitcroft, let alone combine Flitcroft and Linehan to arrive at the features of any one of claims 17 to 22, 25 and 26.

With regard to claim 17, there is no disclosure in Flitcroft of a gateway device that includes a means for transmitting the identifying information to a card-issuing financial institution and for receiving an approval response from the institution over a private data network. Nor is there a disclosure of the gateway device having means to generate a replacement card number upon receipt of the approval response. These features are also not disclosed in Linehan and, therefore, the skilled person would not, as a matter of routine, combine both Linehan and Flitcroft to arrive at claim 17.

With regard to claims 18, 19 and 20, these all depend from claim 17 and, therefore, include the abovementioned features associated with the gateway device. Therefore, claims 18 to 20 are not obvious in view of Linehan and Flitcroft.

With regard to claims 21 and 22, these claims disclose supplementary details of a transaction that are transmitted to the gateway device by the secure data entry device, the supplementary details including one or more of the transaction amount and a merchant identification. Neither of the Flitcroft and Linehan documents disclose a gateway device that receives supplementary details of a transaction transmitted from a secure data entry device. Therefore, the skilled person would not arrive at either of the features of claims 21 and 22 by combining the two U.S. patents.

With reference to claim 25, it includes further identifying features in the gateway device such as a means for receiving payment transaction messages, means for modifying received payment transaction messages and a means for transmitting the transaction messages to the card-issuing financial institution. The gateway device also substitutes actual card numbers for replacement card numbers before transmitting the received payment transaction messages to the financial institution.

As Flitcroft does not disclose a gateway device, let alone a gateway device that has these features, and Linehan only discloses an issuer gateway that also does not include the features of claim 25, the skilled person would not arrive at a combination of features of claim 25 having regard to Linehan and Flitcroft. Therefore, claim 25 is not obvious over these two documents. Finally, claim 26, which is dependent upon claim 17, has the gateway device including a database of replacement card numbers. Neither of Flitcroft or Linehan disclose a gateway device having such a database. Therefore, claim 26 is not obvious over the combination of Flitcroft and Linehan.Linehan attempts to improve the Secure Electronic Transaction ("SET") system. Linehan acknowledges SET as prior art (*see, e.g.*, col. 3, lines 6-10) and discusses SET at some length at column 3, as well as including a diagram of SET (FIG. 1) and noting the various differences between Linehan's system and SET (including how Linehan improves upon SET) at many points throughout the background information provided.

SET is a system for securing online transactions. While SET never succeeded in gaining great popularity, it was designed to function by giving the consumer a digital signature to use online instead of a credit card number, thus hiding the credit card number from the merchant. The signature would be passed to the merchant, who would pass it to their acquiring bank, who would, in turn, pass it onto the issuing bank; the issuing bank would examine the signature and, if it was found to be valid and linked to an account with sufficient available credit, authorize the transaction and pass the authorization back to the acquiring bank, who would in turn pass it to the merchant.

After describing the SET system, Linehan states, at column 3, line 51 onwards:

> Where the wallet servers are run by issuing banks, it would be desirable to have the wallet servers directly authorize transactions before they are submitted to merchants. This would save the time and complexity required when the merchants obtain authorization from issuers through the merchant's acquiring banks. It would also be desirable to expand the cardholder authentication methods supported by the SET protocol, to enable an issuer to independently choose alternate authentication mechanisms without changing the acquirer gateway. As with any system, it would also be desirable to simplify the SET protocol in order to enable its easier implementation and to improve its overall performance.

Linehan then goes on to teach a "4 party protocol" wherein the consumer's PC is connected to both a merchant and the issuer's gateway and the merchant is then connected to the acquirer's gateway. According to Linehan, at column 7, line 14 onwards:

> In this manner, a "thin" wallet is enabled for the consumer in an electronic commerce protocol that is significantly simpler than the SET protocol, and that pre-authorizes payments thereby improving overall performance and enabling greater flexibility for issuer in the authentication of cardholders.

In Linehan, it appears that in most claimed embodiments, communication flow is as follows: it is initiated by the consumer's PC, which communicates with the merchant; the merchant replies to the consumer; the consumer communicates with the issuer gateway; the issuer gateway replies to the consumer; the consumer again communicates with the merchant and finally, the merchant communicates with the acquirer gateway.

Although Linehan states that "Many variations of this 4-party design are possible," the only variation detailed is one where, after the consumer communicates with the issuer gateway, the issuer gateway, rather than replying to the consumer, sends an authorization token to the merchant; the merchant then communicates confirmation to the consumer and subsequently submits the authorization token to the acquirer gateway. In all described network topologies, therefore, Linehan requires direct communication between the consumer and the issuer gateway. Indeed, under "Discussion of the Preferred Embodiment" at column 5, lines 51-54, Linehan states "A principal feature of the invention is providing an issuer gateway and moving the credit/debit card authorization function from the merchant to the issuer thus enabling pre-authorization of payments."

Accordingly, Linehan does not change that basic system utilized by SET to attempt to provide security for on-line transactions. The principal feature which defines both SET and Linehan is the use of a digital certificate, linked to a particular user and account, which is stored in the form of a file on the consumer's computer and sent to third parties to verify the authenticity and payment capacity of the user.

One of the shortcomings of SET and similar systems -- and in applicants' view a principal reason why such schemes failed to gain popular acceptance -- is that they failed to provide

EFTPOS equivalent security, authentication, or functionality. This is due to the above noted principal feature of SET and Linehan system, namely authentication of a user through the transmission of a digital certificate that is linked to a credit account held by a particular user and purports to authenticate that user and which is stored on a personal computer.

The difficulties with using such a method for authentication are multiple. First, the certificate is only as secure as the personal computer (which is notoriously insecure, particularly in the hands of less educated users). An attacker who is able to gain remote control of the computer could easily complete transactions from the user's computer and may well be able to obtain the certificate for future use from other computers.

Second, the certificate must be obtained through means such as applications, conducted outside of the described system, which may be insecure.

Third, the certificate is only linked to one particular account. If a user wishes to use other accounts they must obtain further certificates linked to those accounts through (possibly insecure) applications.

Fourth, such systems only enable the use of credit accounts, not debit accounts, for online transactions. This is because no facility exists for the entry or verification of a PIN, which is a prerequisite enforced by the banking industry for electronic debit transactions. Indeed, given the lack of security of such systems, it is inconceivable that the banking industry would permit them to be used to store or transmit PINs.

It was as a reaction to such software based systems that the present applicants' Point of Pay or "PoP system" was designed. Rather than relying on a software component to try and make an insecure computer to computer transaction more secure, the philosophy behind PoP is to remove the processing and storage of any financial information from the computer altogether. The information is instead processed and transmitted by a separate, purpose made high security data entry device ("PoP Device") which creates its own secure connection to a banking network. The PoP Device has, in the preferred embodiment, a PIN pad and a card reader.

It is true that the PoP Device is, in the preferred embodiment, connected to a computer. However, for the purposes of the transmission of financial information, the computer is merely a "dumb terminal"; no financial or other personally identifying information is ever passed through the computer in an unencrypted form and any attacker would gain no advantage in terms of compromising the PoP system from gaining control of the computer (whether remotely or physically). The security provided by the PoP Device allows definitive authentication of the user and any information transmitted by the Device. This, in turn, allows the PoP system to be connected to the ATM network, as it provides security equivalent to an ATM or store front EFTPOS device.

A key aspect of the PoP claims, therefore, is a secure data entry device that is connected (via a network, such as the Internet) to a financial gateway which is in turn connected to the acquiring bank's financial switch (which forms part of the ATM network).

Aside from the required connections noted directly above, the network topology and communication flow of the PoP Claim, unlike the Linehan system, is highly flexible. While the PoP claim states "the gateway device includes means for transmitting the identifying information to the card-issuing financial institution", it is not necessary (nor envisioned) that the PoP gateway will be directly connected to the issuer's gateway or switch. Rather, the PoP gateway will connect to an acquirer's switch over a private network, which will in turn connect to the issuer's switch over another private network.

Linehan does mention a smart card reader at column 7, line 20. However, there are various substantial differences between a Linehan system with a smart card reader and a PoP system. First, the smart card reader is not a PIN entry device. Accordingly, the Linehan system in this configuration still lacks a means for securely entering and /or transmitting a PIN. Second, a smart card reader, dependent on its design, may not be able to definitively authenticate itself to a gateway. In such an arrangement, the primary authentication would continue to be performed using the digital certificate, including all its inherent flaws. Third, as a result of the lack of security, banking institutions would not permit such a system access to the ATM network and there would be no way to perform debit transactions.

The significant differences between Linehan and Flitcroft et al on one hand and the present invention, as defined in the amended claims, on the other establish that a combination of Linehan with Flitcroft et al does not render the instant claims obvious. In view of these considerations applicant respectfully submits that the rejections should be withdrawn.

CONCLUSION:

The application is believed to be in condition for allowance. Reconsideration of the application is therefore respectfully requested. An early notice of allowance thereof is respectfully solicited. Should the Examiner determine that additional issues remain which might be resolved by a telephone conference, the Examiner is respectfully invited to contact the applicants' undersigned attorney.

Respectfully submitted,

Laurence B. Bond
Registration No. 30,549
Attorney for Applicants
TRASKBRITT, PC
P.O. Box 2550
Salt Lake City, Utah 84110-2550
Telephone: 801-532-1922

Date: December 22, 2010